OLIVIA WHITCROFT

"Every different use of personal data about someone needs a lawful basis"

While the term "lawful basis" may fail to excite, it's a rule that's making the likes of Meta think twice before using your data to train its AI

I'm speaking at a conference in September on "picking the right lawful basis for your processing activity". Don't stop reading! I agree it doesn't sound that enticing, but I promise there is excitement ahead.

Every different use of personal data about someone needs a lawful basis, and you have six options. Your activity must be necessary for a contract with them, a legal obligation, vital interests (life or death), a public task, or legitimate interests. The sixth one is the individual's consent. The tricky thing about consent is that it must be freely given, specific, informed and unambiguous. A tricky part of the others is that word "necessary".

In my preparations, I started rolling out some quick examples for my delegates: "We collect employee PAYE details to send to HMRC" (*easy – legal obligation*). "We use our customers' addresses to send them the product they've bought" (*easy – contract*). "We need property details to calculate Council Tax" (*easy – public task*).

Next, some scenarios that give pause for thought: "We share information with the police to help with investigations." If there's a statutory duty or court order then it's a legal obligation. If not, perhaps legitimate interests, but you need to balance those interests against the interests of individuals. A new lawful basis of "recognised legitimate interests" was proposed under the Data Protection and Digital Information (DPDI) Bill, with no required balancing act. But then an election was called and the Bill was dropped, so its fate is in the hands of our new government and its Digital Information and Smart Data Bill.

"We use customers' email addresses to send newsletters." This could be contract (if part of an agreed service) or maybe legitimate interests; otherwise consent is probably needed. The UK Information Commissioner's Office (ICO) has been in a long-running dispute with Experian about the use of legitimate interests in the context of direct marketing activities (a topic I discussed in issue 351). In April 2024, the Upper Tribunal confirmed the First Tier Tribunal's decision supporting the use of legitimate interests for Experian's activities, highlighting the relevance of benefits to individuals (as well as potential detriments).

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"For consent to be freely given, users must have a real choice"

Finally, I braved some really thorny hot topics. "We use personal data to push targeted adverts based on behaviours" (*hard*). "Personal data is analysed by our artificial intelligence models" (*help!*). How "necessary" are these activities, and is "legitimate interests" even an option? If you seek consent, how can you ensure it is freely given and informed?

Meta has tried them all

Meta has had a tough time finding a lawful basis for its behavioural advertising activities on Facebook and Instagram in the EU. When the GDPR first arrived, it sought to rely on such advertising being necessary for a contract (for services) between Meta and the user, based on the terms of service. However, this faced the challenge that behavioural advertising is not objectively necessary to provide its social networks. In 2023 it put forward legitimate interests: a positive user experience and generating revenue (from advertising payments), among others. This was contested on the basis that the interests of users overrode Meta's interests.

The challenges culminated in a binding decision of the European Data Protection Board in October 2023, instructing the Irish Data Protection Commission (DPC, Meta's lead EU supervisory authority) to ban Meta's use of data for behavioural advertising on the basis of contract or legitimate interests, which the DPC did by an enforcement notice in November 2023.

So Meta changed its lawful basis to consent. For consent to be freely given, users must have a real choice. If saying "no" means you're denied access to Facebook, a prominent global platform with over three billion monthly active users, then you're being strongly pushed towards consenting, and it isn't really freely given. Instead, Meta adopted a "consent or pay" model. If you don't want to receive the personalised adverts, then you can pay a monthly fee for access to the service.

The EDPB once more put their heads together and, in April 2024, adopted an Opinion on this model in the context of large online platforms such as Facebook. Its view is that consent cannot be said to be freely given, as users will still be under pressure to consent, where the alternatives are either not to access the service or to pay a (possibly disproportionate) fee. There needs to be an equivalent alternative for those who don't consent, such as perhaps receiving adverts that are not based on analysis of personal data. In July 2024, the European Commission gave the view that Meta's model was also in breach of the EU Digital Markets Act (which requires large players in the digital sector to play fairly).

BELOW Experian has been involved in a long-running dispute with the ICO

UK consent or pay

In March 2024, the ICO called for views on "consent or pay" business models in the UK market. It considers that, in principle, data protection law doesn't prohibit these models. But it outlined four areas to consider in assessing whether a consent is valid: the power balance between platform and user; the equivalence of the ad-funded

service to the paid-for service (so without "premium extras" if you pay); an appropriate fee; and privacy by design, including clear and equal presentation of the choices.

So let's say you're a small platform, with plenty of competitors and choice for users. In order to keep running, you need a source of income. You calculate the revenue you would receive from targeted advertising and work out an equivalent service fee. You then clearly present users with two options to access the platform: consent to behavioural advertising or pay the service fee. On the face of it, this seems similar to Meta's model. But your low market power, fairly calculated fee and clarity over the options could lead to freely given consent in this context.

AI and legitimate interests

In May 2024, it was reported that HMRC was hiring customer services personnel using AI, without the applicant ever speaking to a human. This implied the AI was analysing personal data and making recruitment decisions. I scoured the web trying to find a privacy notice identifying HMRC's lawful basis for these activities, to no avail. So I made a freedom of information request to try to find out. My initial request was lost in the ether, so there was a delay in HMRC pressing "Go" on its stopwatch for the 20-day response period. I then received a fairly cryptic response that was silent on lawful basis, but seemed to say AI wasn't used in the process to the extent reported. Now I'm grumpy that I'm no further forward on this.

There are (at least) two key processing activities to consider in using AI models in this way. First, the use of personal data to train the model. You may, for example, use data about good performers among your existing employees to train the AI what to look for. Second, the AI will process personal data about applicants to assess suitability for the role and potentially make the decision whether to recruit.

Training the model

An interesting decision of the Belgian data protection authority in March 2024 concerned the use of personal data to train a data model. An English-language summary and machine translation has been reported in GDPRhub (**gdprhub.eu**) run by the privacy rights group NOYB (**noyb.eu**). The authority decided a bank could rely on legitimate interests to use customer transaction data to train its model offering tailored customer discounts. Building the model for this marketing purpose was a legitimate interest, and analysis of transaction data was necessary to achieve it. The balancing test took into account that the model involved low-risk data, it wasn't used to identify customers, and no personal data was shared externally.

The ICO also envisages the use of legitimate interests as a lawful basis for training models in its AI guidance. It flags the need to properly define the purposes and justify use of each type of data. An organisation must demonstrate that the range of variables and models it intends to use is a reasonable approach to achieving the outcome. The mere possibility of usefulness is not enough to be "necessary". Assessments may need to be re-visited over time as purposes are refined, or if an individual exercises their right to object to processing based on legitimate interests.

And, of course, Meta is at the forefront of this as well. In June 2024, it updated its privacy notice to include use of user data to train generative AI technology, on the basis of legitimate interests. But NOYB immediately filed complaints with 11 EU data protection authorities. In the UK, the ICO has asked Meta to "pause and review" its plans.

ABOVE **Meta has struggled to find a lawful basis for its ads on Facebook and Instagram**

Deployment of AI

Deployment of AI should be considered separately. If the AI is making a decision without human involvement and which significantly affects an individual (such as whether to recruit them, offer them a loan or give them access to a service), then this is only lawful if the decision is necessary for a contract with the individual (or for entering into a contract), required or authorised by law, or based on explicit consent. So legitimate interest is not available. Though it is another area that was set to be relaxed under DPDI, and we await to see whether this is revived.

"You need to pick the right activity, and the lawful basis will fall into place with it"

BELOW **HMRC has reportedly used AI to hire staff**

Both the EDPB and ICO have provided examples of using solely automated decision-making to sift through large numbers of applications during a recruitment process, but the guidance on lawful basis doesn't appear clear or consistent. And real-life examples are surrounded in mystery, such as the HMRC story. The EDPB indicates that the sifting process can be considered necessary for entering into the employment contract. The ICO says that the contract basis can only be used at the job offer stage, so is it implying that explicit consent may be an option at an earlier stage? Consent needs to be informed and freely given, so individuals must have clear information about the role of the AI, and an option to say "no" (without being put at a disadvantage).

For AI that doesn't make such decisions (or if there is meaningful human involvement), legitimate interests could be considered, and the balancing test is needed. Factors such as the quality of training data and the risk of bias should be factored into this.

Data protection by design

Coming back to the title of my conference presentation, I think it's topsy-turvy. It's not a matter of deciding what you're going to do and then picking the right lawful basis. That way, you may be unable to find one at all, as Meta is finding with its behavioural advertising activities, or if you leap into using AI to make significant decisions. Data protection by design means designing what you're going to do in line with data protection rules and rights. So, rather than picking the right lawful basis, I think you need to pick the right activity, and the lawful basis will fall into place with it.

olivia.whitcroft@obep.uk